

FIG.1

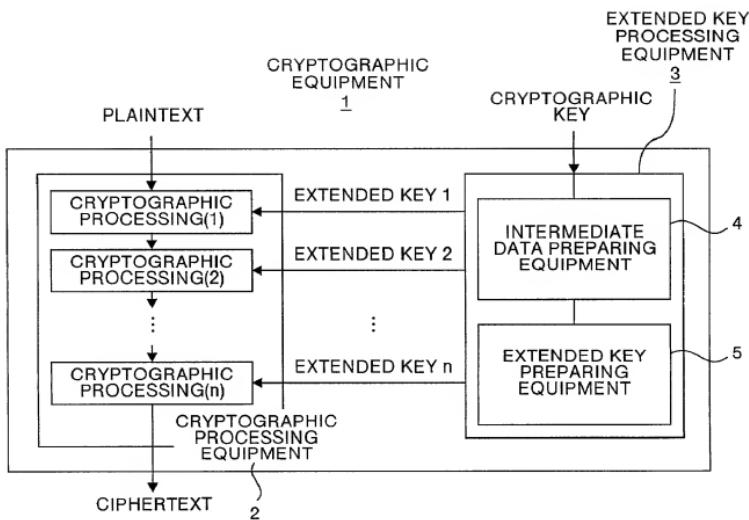


FIG.2

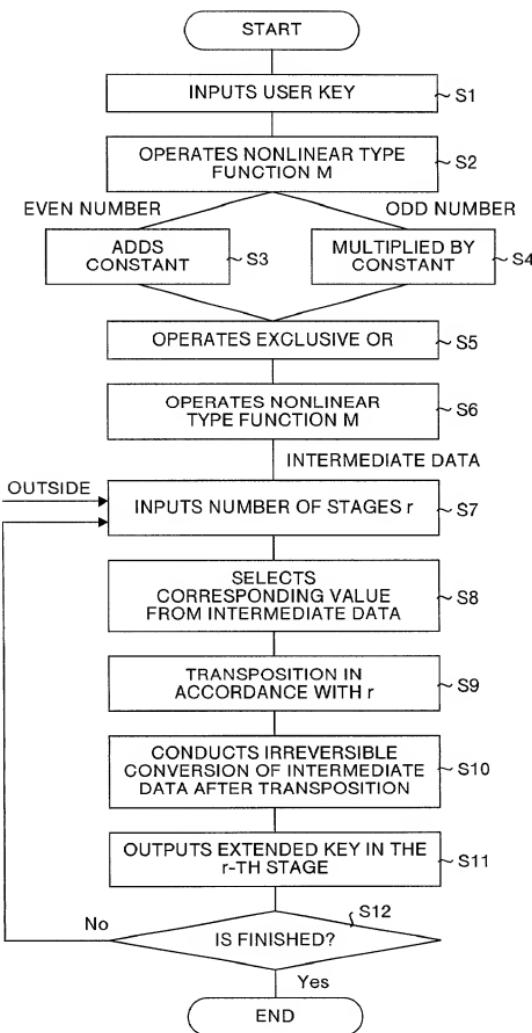


FIG.3

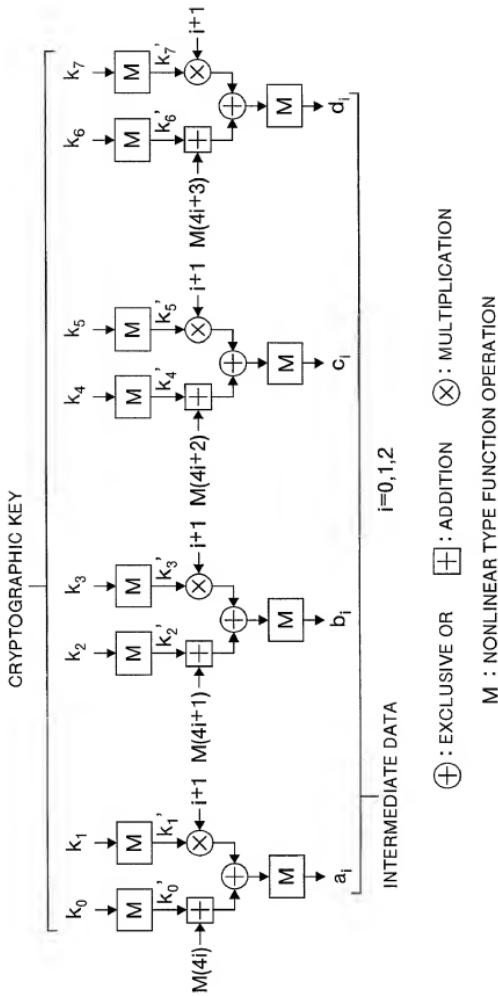
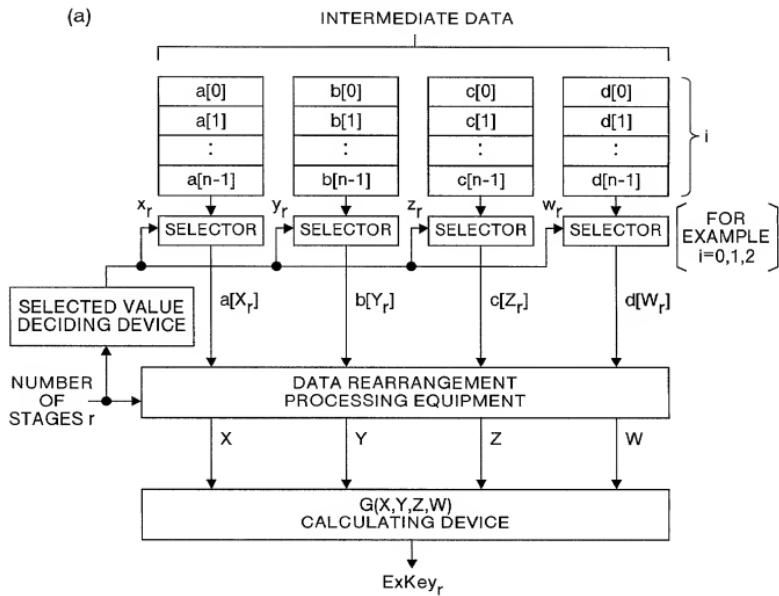
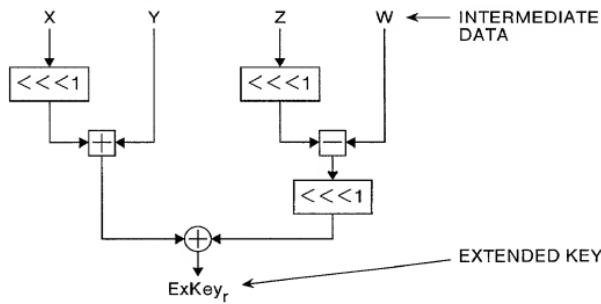


FIG.4

(a)

(b)  $G(X, Y, Z, W)$  CALCULATING DEVICE $\boxed{+}$ : ADDITION $\boxed{-}$ : SUBTRACTION $\boxed{\oplus}$ : EXCLUSIVE OR $\boxed{<<<1}$ : LEFTWARD CYCLICAL SHIFTING BY 1 bit

## FIG.5

(a)  $x_r = z_r = r \bmod 3, \quad y_r = w_r = r + [r/3] \bmod 3 \quad \dots \text{EQUATION (1)}$

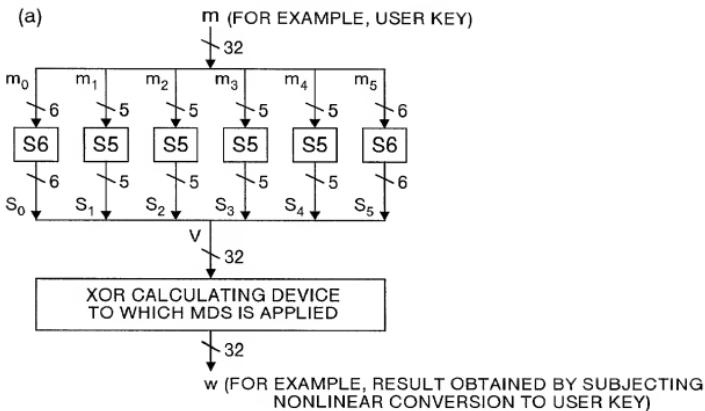
(b) CIRCULATING WITH 9 ELEMENTS

r	0	1	2	3	4	5	6	7	8	9	0	...
Xr	0	1	2	0	1	2	0	1	2	0	1	...
Yr	0	1	2	1	2	0	2	0	1	0	1	...
Zr	0	1	2	0	1	2	0	1	2	0	1	...
Wr	0	1	2	1	2	0	2	0	1	0	1	...

(c) ORDER TABLE

r (-TH STAGE)	ORDER_12(X,Y,Z,W,r)	REARRANGEMENT
0	(X,Y,Z,W)	
1	(Y,X,W,Z)	
2	(Z,W,X,Y)	
3	(W,Z,Y,X)	
4	(X,Z,W,Y)	
5	(Y,W,Z,X)	
6	(Z,X,Y,W)	
7	(W,Y,X,Z)	
8	(X,W,Y,Z)	
9	(Y,Z,X,W)	
10	(Z,Y,W,X)	
11	(W,X,Z,Y)	

FIG.6

(b)  $S_5(x)$ 

x	$S_5(x)$	x	$S_5(x)$	x	$S_5(x)$	x	$S_5(x)$
0	20	8	22	16	27	24	23
1	26	9	30	17	11	25	5
2	7	10	13	18	1	26	8
3	31	11	14	19	21	27	3
4	19	12	4	20	6	28	0
5	12	13	24	21	16	29	17
6	10	14	9	22	2	30	29
7	15	15	18	23	28	31	25

(c)  $S_6(x)$ 

x	$S_6(x)$	x	$S_6(x)$	x	$S_6(x)$	x	$S_6(x)$
0	47	16	37	32	62	48	3
1	59	17	63	33	52	49	16
2	25	18	20	34	35	50	41
3	42	19	61	35	18	51	34
4	15	20	55	36	14	52	33
5	23	21	2	37	46	53	7
6	28	22	30	38	0	54	45
7	39	23	44	39	54	55	49
8	26	24	9	40	17	56	50
9	38	25	10	41	40	57	58
10	36	26	6	42	27	58	1
11	19	27	22	43	4	59	21
12	60	28	53	44	31	60	43
13	24	29	48	45	8	61	57
14	29	30	51	46	5	62	32
15	56	31	11	47	12	63	18

FIG.7

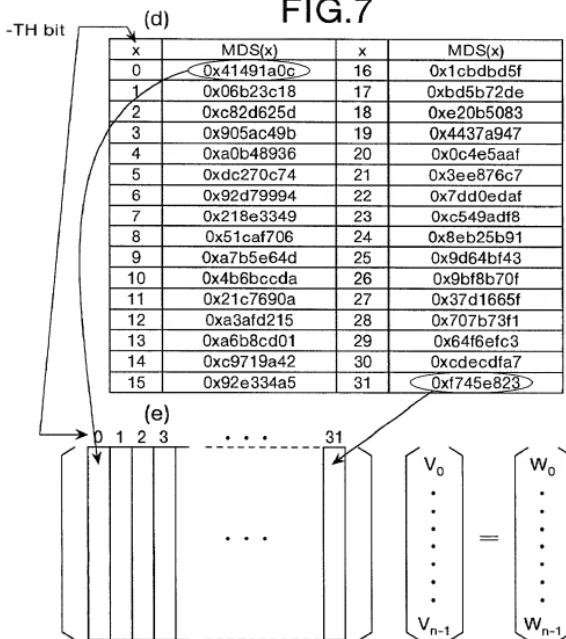


FIG.8

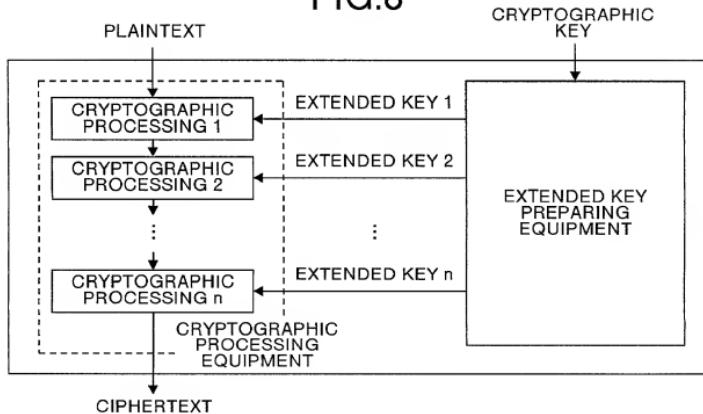


FIG.9

